DOMAIN: SECURITY

# DISCIPLINE: Host Protection

## Discipline Roadmap for: Host-based Intrusion Prevention System (HIPS)

| Current | 2 Years | 5 Years |
|---|---|---|
| **Baseline Environment** | **Tactical Deployment** | **Strategic Direction** |

McAfee Entercept

Symantec

Cisco

ISS

Sana

AppArmor (Linux)

### Strategic Direction

Market Watch of a single multi-function threat management client.

| Shared | Agency |
|---|---|
|  | ✓ |

### Retirement Targets

N/A

### Mainstream Platforms (must be supported)

McAfee Entercept, Symantec, Cisco, ISS, Sana, AppArmor

### Containment Targets

N/A

### Emerging Platforms

Consolidation into a single multi-function threat management client.

### Implications and Dependencies

- Centralized management and administration of host-based clients.
- It is highly recommended that multiple products be used in concert in order to create an in-depth defense since not all products defend equally.

### Roadmap Notes

- Certain products listed may be better suited for server or desktop dependent on use-case.
- Must support the SC Enterprise Architecture standards for networking (LAN, WAN, etc.)

# DISCIPLINE: Host Protection

## Discipline Roadmap for: Host-based Intrusion Prevention System (HIPS)

- **Discipline Boundaries:**
  - An IPS is any device which exercises control to protect networks, applications and computers from exploitation. IPS are intended to resolve ambiguities in passive network monitoring by placing detection in-line. There are 4 basic types of IPS: host-based network, content-based, and rate-based (the last 3 are addressed in a separate roadmap). Host-based IPS (HIPS) systems reside on a specific IP address, such as a PC system.
- **Discipline Standards:**
  - Currently, there are no HIPS specific standards.
- **Migration Considerations:**
  - None
- **Exception Considerations:**
  - Specialized business needs requiring exception should be reviewed through the AOC exception process.
- **Miscellaneous Notes:**
  - None
- **Established**
  - November 15, 2006
- **Date Last Updated:**
  - November 15, 2006
- **Next Review Date:**
  - November 2007